UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with email account practical_75@hotmail.com that is stored at premises controlled by Microsoft Corporation.

Case No. 18-M-123 (DEJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Section 2339B(a)(1).

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Scott Mahloch
Printed Name and Title

Sworn to before me and signed in my presence:

Date: Aug. 9, 2018

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones, U.S. Magistrate Judge
Printed Name and Title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ACCOUNT PRACTICAL_75@HOTMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION	Case No. 18-M-123 (DEJ)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Scott Mahloch being duly sworn, hereby depose and state the following:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for information associated with email account practical_75@hotmail.com (the ACCOUNT) that is stored at the premises controlled by Microsoft Corporation (Microsoft), an email provider headquartered at 1065 La Avenida, Building 4, Mountain View, California (CA) 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since April 2009. I am currently assigned to the Joint Terrorism Task Force at the Milwaukee Field Office, where I conduct a variety of investigations in the area of

counterterrorism in the performance of my duties. I have investigated and assisted in the investigation of matters involving violations of federal law related to domestic terrorism, international terrorism, weapons of mass destruction, the distribution of bomb-making materials, and material support, including in the preparation and service of criminal complaints and search and arrest warrants. I have conferred with colleagues who have received specialized training from the FBI in investigating crimes related to explosives, biological weapons, and weapons of mass destruction.

3. The statements contained in this affidavit are based in part on my personal knowledge, as well as on information provided to me by other law enforcement officers and civilians. This affidavit is being submitted for the limited purpose of securing the requested search warrant, and I have not included each and every fact known to me concerning this investigation.

4. Based on facts set forth in this affidavit, I submit there is probable cause to believe that WAHEBA ISSA DAIS has attempted to provide material support to a foreign terrorist organization in violation of Title 18, United States Code, Section 2339B(a)(1). DAIS is also known by an alias referred to here as "HE." On June 13, 2018, DAIS was charged by criminal complaint with attempting to provide material support or resources to ISIS, in violation of 18 U.S.C. § 2339B(a)(1). On June 26, 2018, DAIS was indicted on two counts of this same crime. I submit there is also probable cause to search the subject DEVICES for evidence, fruits, and instrumentalities of this crime.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. § 2339B, relating to attempting to provide material support and resources to an FTO. Elements of the offense are the following: The defendant knowingly attempted to provide material support or resources to a designated FTO; the defendant knew that the organization was a designated foreign terrorist organization, that the organization had engaged in or was engaging in terrorist activity or terrorism; and one of the five jurisdictional requirements is satisfied.

THE ISLAMIC STATE OF IRAQ AND AL-SHAM

7. On or about October 15, 2004, the United States Secretary of State designated Al-Qaeda in Iraq (AQI), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization (FTO) Under Section 219 of the Immigration and Nationality Act and Specifically Designated Global Terrorist under section 1(b) of Executive Order 13224.

8. On or about May 15, 2015, the Secretary of State amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and Specifically Designated Global Terrorist under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant (ISIL) as its primary name. The Secretary also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (ISIS—which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria (ISIS), ad-Dawla al'Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On

September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

BACKGROUND OF INVESTIGATION AND FACTS ESTABLISHING PROBABLE CAUSE

8. The FBI Joint Terrorism Task Force has been investigating WAHEBA ISSA DAIS (DAIS) as a suspect involved in the provision of material support to ISIS, in violation of 18 U.S.C. § 2339B. The investigation has revealed that DAIS, through the use of multiple social media accounts that she has hacked and taken over from unwitting victims and private social media platforms, promotes ISIS ideology, recruits adherents to ISIS, advocates that her followers conduct attacks in the name of ISIS, collects information on how to make explosives and biological weapons and on how to conduct terrorist attacks, and distributes that information to individuals so they can conduct attacks on behalf of ISIS. For instance, DAIS used one of her pro-ISIS Facebook accounts (an account she hacked and took over from an unwitting victim) to direct an individual, whom she believed to be an ISIS supporter planning to conduct an attack in the name of ISIS, to her password-protected social media channel to find instructions on how to make Ricin and then suggested the individual introduce the Ricin to a government post or water reservoirs.

9. According to information provided by the Department of Homeland Security, DAIS was born on or about August 22, 1972, in Jerusalem, Israel, and was allowed to enter the United States without a passport arriving in Chicago, Illinois (via Paris, France), in approximately November 1992 because of her marriage to a U.S. Citizen (her husband filed for divorce in 2003). On DAIS's visa application, she indicated she intended to stay in the United States permanently as a housewife; that she was from Jerusalem; and that she could speak, read, and

write in English and Arabic. DAIS is now a Lawful Permanent Resident of the United States and lives in Cudahy, Wisconsin, with five of her children, including three minors.

10. The FBI's investigation indicates that DAIS uses multiple Facebook, Twitter, identified social media, and email accounts that contain pro-ISIS statements and information on how to make biological weapons, explosives, and explosive vests. As explained in more detail below, information provided by Facebook pursuant to 18 U.S.C. § 2702 in approximately January 2018 revealed that a Facebook user with an identified screen name (referred here to as HE) and User Identification number (UID) ending in 1813 appeared to be a Wisconsin-based user posting detailed instructions on how to make explosive vest bombs in support of ISIS. This Facebook user also appeared to be engaged in detailed question and answer sessions discussing substances used to make bombs. As also discussed more fully below, FBI investigation has determined this user was DAIS. Further investigation has revealed that DAIS has used multiple social media platforms to pledge allegiance to ISIS, promote ISIS's terrorist agenda, communicate with ISIS members overseas, facilitate and encourage recruitment and attack planning for ISIS, and distribute instructions on explosives and biological weapons to self-proclaimed ISIS members and to people she believed to be planning to conduct attacks on behalf of ISIS. The investigation has revealed that DAIS hacks Facebook accounts, taking them over from unwitting victims and changing the profile picture, friends list, and display name. FBI investigation has identified the following Facebook accounts as being used by DAIS to attempt to provide material support to ISIS, distribute information on bomb-making and recipes for Ricin, and facilitate attacks: UID ending in 1813, UID ending in 4063, UID ending in 2942, and UID ending in 6059. These four accounts are not an exhaustive list of all the accounts DAIS has hacked and taken over as her own.

11. Based on the FBI investigation, I believe that DAIS, who has pledged her allegiance to ISIS, is actively promoting ISIS propaganda through social media channels in an attempt to radicalize and recruit ISIS members and to encourage ISIS supporters to conduct terrorist attacks. I further believe that DAIS has helped facilitate planning for attacks in the United States on behalf of ISIS and overseas by providing instructions on how to make explosives, biological weapons, and suicide vests, and providing detailed instruction to people interested in attacks and attack planning. DAIS has also expressed a personal desire to travel overseas in support of ISIS.

DAIS'S HACKING OF VICTIM FACEBOOK ACCOUNTS

12. Open source searches and information provided by Facebook pursuant to 18 U.S.C. § 2702 indicate that DAIS and the individuals who are communicating with DAIS on Facebook are using hacked Facebook accounts as a way to avoid law enforcement detection of their communications. When DAIS takes over a Facebook account, she changes the display name to a variant of HE (written in English and/or Arabic) and changes the profile picture. The profile picture used by DAIS on these hacked Facebook accounts was taken by a professional photographer and is of a young girl wearing a blue dress. The photograph was taken as part of a series documenting Yazidi, a minority population in northern Iraq, fleeing their hometown to escape violence caused by the Islamic State militants. This photograph can be found on the internet.

13. On or about January 11, 2018, an FBI confidential source (Source #1)[1] reported that DAIS is unemployed and has her Islamic husband (which means married by their religion and not law) pay the bills. Source #1 described DAIS as constantly on social media promoting ISIS and using

[1] Source #1 was opened in approximately January 2018. Some of his/her reporting has been corroborated, he/she has direct access through a sub-source, and he/she is considered reliable. To date, Source #1 has not been paid and is motivated by not wanting to lose his/her ability to obtain a Top Secret clearance for employment due to his/her association with the subject. Source #1 was applying for a position that required a TS clearance.

an identified social media application to talk to "shady people" in the Middle East on a regular basis. Source #1 reported that DAIS uses accounts on Twitter and Facebook, but they are always being shut down due to her posting pro-ISIS propaganda. According to Source #1, DAIS also has numerous "throw away" e-mail addresses to create all these accounts. Source #1 stated that DAIS has a YouTube account that she subscribes to and possibly creates videos on how to hack into social media accounts and is able to crack passwords for Facebook accounts. As discussed below, FBI investigation has confirmed that DAIS hacks into Facebook accounts belonging to others, as an operational security measure, and uses those accounts to promote ISIS and to facilitate ISIS recruitment and attack planning.

14. The FBI's investigation has identified multiple Facebook accounts hacked by DAIS. The following list of accounts includes examples of the multiple accounts and is not exhaustive. The information below was provided to the FBI pursuant to legal process, publicly available information, and open source research.

15. Review of account information received pursuant to legal process shows that Facebook account with UID ending in 1813 and display name (HE) was used to pass information on how to build explosives to members of ISIS. FBI investigation has revealed that the account previously belonged to an unrelated female (Victim No. 1) but was hacked and taken over by DAIS in approximately January 2018. According to Facebook, UID ending in 1813 was created in approximately January 2012 by a female in Carabobo, Venezuela. On or about January 4, 2018, the account's display name was changed to HE and the majority of the original friends were removed from the account. The same day, the account quickly began to add a large number of new friends. The account profile picture used was the distinct photo of the young girl in a blue dress that was previously discussed. After the account name was changed, it was frequently accessed

from an Internet Protocol (IP) address that resolved to DAIS's residence. It is noted that on or about January 8, 2018, while using UID ending in 1813 to exchange private messages, DAIS provided email address baqyyia22@gmail.com as a means to contact her outside of Facebook. At that time, this email address was associated with DAIS and a phone number that was subscribed to by DAIS. Based on prior investigation and source reporting, I believe DAIS is the user of UID ending in 1813.

16. On or about January 23, 2018, investigators conducted an open source search of DAIS's alias, HE, and identified UID ending in 4063, which also appears to have been hacked and taken over from a female in Venezuela (Victim No. 2). My review of publicly available information on this account revealed it had the same distinct profile picture as UID 1813. The account was previously used by a female whose profile showed she studied at a University in Carabobo, Venezuela. Review of account information received pursuant to legal process shows this account was created in approximately January 2012, and on or about January 8, 2018, the friends from the original account were removed. On or about January 23, 2018, the account name was changed to a variant of HE and new friends began to be added. After the name of the account was changed, it was accessed frequently from an IP address that resolved to 3441 Cudahy Avenue, Cudahy, WI, which is DAIS's residence. Based on prior investigation and source reporting, I believe DAIS is the user of UID ending in 4063.

17. On or about March 2, 2018, an FBI Undercover Employee (UCE) looked up Facebook user name HE and discovered Facebook account with UID ending in 2942 with that name and DAIS's distinct profile picture. The UCE's review of UID ending in 2942 showed the subscriber is from Venezuela (Victim No. 3). The UCE sent DAIS a private message, asking for advice and DAIS provided email address baqyyia22@gmail.com to the UCE as her email address. Google's

response to legal process also indicated that the email address baqyyia22@gmail.com was primarily accessed from an IP address that resolves to DAIS's residence. Based on the foregoing, I believe DAIS used Facebook account UID ending in 2942.

18. On or about April 23, 2018, investigators conducted an open source search of HE in Arabic and identified Facebook account UID ending in 6059 under the display name of a variant of HE The account had the same distinct profile picture that DAIS is known to use. The profile indicates the subscriber is from Camp Grande, Brazil, and includes pictures of a young male. The rest of the account is in Arabic. IP address records obtained via Grand Jury subpoena indicate that the IP address used to access the account resolved to 3441 Cudahy Avenue, Cudahy, WI. I believe that this account was previously used by Victim No. 4 and then hacked by DAIS on or about April 12, 2018, when the cover photograph was changed to DAIS' distinct photograph.

DAIS'S PLEDGES OF SUPPORT TO ISIS

19. DAIS has pledged her allegiance to ISIS on numerous occasions. On or about February 12, 2018, DAIS (using Facebook UID ending in 4063) posted on her Facebook wall, confirming that her posts are her beliefs and that she believes in the doctrine of ISIS: "#Caution. When I publish any statement I completely believe in it. I was and I continue to be on the doctrine of the Islamic State." DAIS (using Facebook UID ending in 4063) posted on her Facebook wall on or about February 10, 2018, a post titled "#Renewal of the pledge of allegiance one more time." DAIS wrote, "I pledge allegiance to Ameer al Mumineen [the commander of the faithful] Ibrahim al-Husaini al-Qarashi, [Abu Bakir al-Baghdadi] to listen and obey in what is desirable and undesirables and in times of hardship and prosperity, and to endure being discriminated against and to not dispute the orders of those in charge, unless I witness a clear apostasy, for

which Allah has shown me a clear proof, and Allah is my witness." In response to this post, seventeen of her friends commented pledging their allegiance to ISIS as well.

20. A review of information provided from Facebook pursuant to 18 U.S.C. § 2702, identified a conversation on or about January 7, 2018, between DAIS (using Facebook UID ending in 1813) and another self-proclaimed ISIS supporter (referred to here as AK) in which they discussed allegiance to ISIS and traveling to join ISIS. DAIS claimed she was born in the United States and was living there. She told AK that she had pledged allegiance to ISIS and was seeking a way to join ISIS in Syria but is forbidden from leaving the country. She further informed AK that an ISIS military trainer in Raqqa, Syria, was trying to assist her in getting to Syria via Turkey. DAIS declared she follows the path and ideology of the Islamic State and that she would not bow for any tyrants. She stated this numerous times throughout the conversation with AK. AK declared that he is a supporter of ISIS as well.

21. In this same conversation, DAIS told AK that she wanted to leave America, but could not and if she tried to leave, she would be arrested for "conspiracy to join." DAIS said that she prayed that Allah would facilitate her exit and that she may "try in a few months." AK told her that they "may end up in Paradise." DAIS told AK that she knew some brothers from Diwan (believed to refer to the ISIS Ministry) and that she had inquired and learned that she can travel to join ISIS without a male escort, which she did not have. DAIS stated she had an ISIS contact in Al-Raqqah who had told her to travel to Turkey and that he would arrange for a male escort to meet her, but then the individual left for Al-Barakah and was "martyred." She said that she had seen videos of him training soldiers online.

22. DAIS has pledged her allegiance to ISIS and has been praised by others for her online support of ISIS via Facebook account UID ending in 1813. For instance, on or about January 5,

2018, a Facebook user (referred to as AA) sent DAIS a private message that stated, "All your postings are in the service for Jihad and the Mujahidin. God bless you." On or about January 14, 2018, DAIS exchanged private messages with the user of Facebook UID ending in 4904 (referred to as AS) about restoring Facebook accounts that had been suspended. DAIS said, "May God keep you safe" to which AS responded, "and may you stay with us on Facebook forever." DAIS said, "except…May God grant me martyrdom and I leave the Facebook." AS responded by telling DAIS that "we are in jihad to spread this message and the truth. As long as the message is God you will be rewarded... all of us wish for and ask God to grant us martyrdom." On or about January 24, 2018, DAIS (using Facebook UID ending in 4063) posted on her Facebook wall urging people to add #The_Supporters_Campaign to their friends list. The user of another Facebook account (Facebook User No. 7) responded by declaring DAIS a supporter of ISIS and very knowledgeable.

DAIS'S PROMOTION AND RECRUITMENT ACTIVITIES ON BEHALF OF ISIS

23. DAIS has used social media on multiple occasions to promote ISIS and its terrorist agenda and to attempt to recruit others to join ISIS and to commit attacks on behalf of ISIS. On or about January 30, 2018, the UCE conducted an open source search of DAIS's alias, HE, and identified Facebook account UID ending in 4063. Subsequently the UCE sent a friend request to that account and it was accepted that day. The UCE then was able to view the Facebook wall of UID ending in 4063. The UCE noted that DAIS had posted the following in Arabic: "#Attention to the non-#supporters brothers: I accepted your friend requests hoping that Allah will guide at least one of you [to become a supporter]."

24. On or about February 24, 2018, DAIS (using Facebook UID ending in 2942) posted a link to a social media channel entitled, "Khilafah Ray for Supporters Group." I believe Khilafah refers to the Caliphate, also known as ISIS. The UCE visited the channel on February 26, 2018, and noted that the page had multiple voice messages posted by DAIS's social media account @ISWarrior and they consisted of Jihadi songs and speeches by ISIS leaders. One of the messages encouraged ISIS supporters who cannot travel to ISIS-controlled areas to conduct terrorist attacks in the countries where they reside. If military targets are not in their reach, then attacks directed at civilians are even more desirable by ISIS.

25. On or about January 23, 2018, DAIS (using Facebook UID ending in 4063) posted on Facebook that her social media channel, "The Caliphate's Ray," had been removed. She then posted links to two social media channels. A Facebook user (referred to here as II) posted that it suits DAIS well to be the press manager for ISIS. II continued to praise DAIS for her perseverance, efforts, and exemplary support of ISIS.

26. A review of information provided from Facebook on or about February 6, 2018, pursuant to 18 U.S.C. § 2702, identified a Facebook user (referred to here as OG) who was planning a potential ISIS attack and had been communicating with DAIS (using Facebook account with UID ending in 4063) about the attack. On or about January 26, 2018, OG asked DAIS if she knew about Sharia. DAIS responded by stating that OG should ask the question and DAIS would send it to an expert for an answer. OG stated that he would be traveling to France. He then said it would be better to die than rot in prison. He asked how he can take revenge for ISIS. He suggested running a car through people or shooting at people. He then asked how he would be judged by God after killing many people. DAIS responded that she will send him an answer

later. On or about January 27, 2018, DAIS sent a link to a Facebook profile (referred to here as SM) and told OG to talk to this individual, that he will be beneficial to OG.

27. On or about January 28, 2018, OG and SM exchanged private Facebook messages. OG said he was a 25-year-old Algerian who had previously discussed plans with HE (using a short form for DAIS's alias) to travel to France. He said he wanted to plan an operation in support of ISIS so DAIS suggested he talk to SM. SM then sent OG the following pledge to ISIS: "Renewal of the pledge of allegiance, we are renewing the pledge of allegiance to Sheikh Abu Bakr Al-Bughdadi [sic] to obey him in everything, not to go against his will, not to flee during the fight, not to deny the religion of God and God is our witness." OG requested weapons and brothers to help with his attack. SM reminded OG that the work is individual. On or about January 30, 2018, OG sent DAIS a message saying that DAIS is really knowledgeable.

DAIS'S DISTRIBUTION OF EXPLOSIVES & BIOLOGICAL WEAPONS INFORMATION

28. DAIS has distributed information pertaining to explosives and biological weapons on Facebook and other social media platforms in the form of videos and conversations about bomb-making and biological weapons materials. In particular, DAIS has used Facebook UID ending in 1813 to distribute information on how to build explosives and biological weapons so that people who want to commit violent acts in the name of ISIS will use this information to commit acts of violence. DAIS promotes violent acts in the name of ISIS on her Facebook pages to her Facebook friends who are self-proclaimed ISIS members and supporters. For instance, one friend of account ending in UID 1813 (Facebook User No. 8) has instructions for creating explosives and Ricin on his page and photographs that include the ISIS flag. On or about January 16, 2018, another friend of this account (Facebook User No. 9) engaged in a private message conversation with DAIS (using Facebook UID ending in 1813) in which he said he had been with ISIS for

years and told her about specific battles and described the battlefield in detail. As described above, in a private message conversation with DAIS (using Facebook UID 1813), AK declared that he is a supporter of ISIS as well.

29. DAIS has posted numerous videos about explosives on Facebook. On or about January 8, 2018, DAIS posted a video on her Facebook page with UID ending in 1813. The video is a presentation from "Sawt al-Jihad" (translated as "The Voice of Jihad") and titled, "Explosive Belt/Vest." The video purports to provide step-by-step instructions on how to make an explosive belt and then demonstrates the effect of the bomb when it explodes. Audio in the background plays a chant in support of Jihad. On or about January 11, 2018, DAIS posted a video on the Facebook page for UID ending in 1813. The video is titled, "The Practical Training in the Making of Ammonium Nitrate." The video purports to provide step-by-step instructions on how to make Ammonium Nitrate. On or about January 11, 2018, DAIS posted a video on the Facebook page for UID ending in 1813. The video is titled, "The Practical Training in the Making of TNT."[2] The video purports to provide step-by-step instructions on how to make TNT. Audio in the background plays a chant in support of jihad.

30. DAIS continually seeks to collect information on the best explosives and biological weapons techniques in order to pass this information on to would-be ISIS attackers. On or about January 8, 2018, DAIS used Facebook UID ending in 1813 to communicate with a Facebook user (referred to here as AO) about explosive vests. AO told DAIS that ISIS made a safer and more reliable explosive belt. AO explained that they do not use electronic detonators because they are dangerous and may explode prematurely and suggested a grenade with a fuse. DAIS asked if he had any videos or written instructions that he could share with her. AO then began to

[2] I know that TNT is Trinitrotoluene, a chemical compound that is a high explosive.

discuss plans to kill Jews overseas. At that point, DAIS suggested that AO not discuss such topics on Facebook because they are probably being monitored.

31. On or about January 9, 2018, DAIS (using Facebook UID ending in 1813) had a detailed conversation with AK about substances used to create bombs. On or about January 9, 2018, DAIS posted on her Facebook wall that Nitric Acid[3] can be found in gold stores but that a clearance is required to purchase it. DAIS recommended producing it because it is difficult to purchase. She then asked where it can be purchased in the Arab Peninsula. She proceeded to ask for the names of commercial fertilizers that would not trigger suspicion when asked about. She posted within the comments that she had heard that nitric acid is used to melt gold so she wanted to know if it could be purchased from gold stores and if that would raise suspicion. DAIS then asked that someone try to purchase nitric acid from a pharmacy after someone suggested it could be purchased that way. DAIS also recommended researching where to get instant fertilizer in Western countries. She then asked if there are nitrates in Potassium Nitrate. AK responded that Ammonium Nitrate[4] needs to be extracted from fertilizer because it is sold in large quantities to land owners. He recommended that this would make a good security cover. If asked questions, AK suggested that DAIS say she does not understand chemicals but is merely a farmer.

32. DAIS has attempted to provide material support to ISIS by providing detailed instructions on how to make Ricin to an individual seeking to commit an attack in the name of ISIS.

33. In particular, on or about March 2, 2018, the UCE sent a private message to DAIS (using Facebook UID ending in 2942) requesting her permission to discuss a sensitive and important

[3] I know that Nitric Acid is a strong acid chemical compound that carries oxygen atoms. It can be used to oxidize or provide oxygen to other chemicals utilized in explosives.
[4] I know that Ammonium Nitrate is a chemical compound that is a strong oxidizer often used in explosives.

topic that the UCE needed her opinion on. DAIS thanked the UCE for his/her confidence and trust. She encouraged the UCE to share his question. The UCE told DAIS that he/she had anticipated completing his/her master degree in a year, but could no longer stand living in the land of the infidel. The UCE stated he/she constantly clashed with colleagues and felt that government spies were everywhere. DAIS responded saying, "I am reading your words and unfortunately, you are causing your own demise by clashing with them. We live in a time where you do not know when you are going to be stabbed in the back. And I don't think the Islamic State would want its supporters be thrown in infidels' prisons. We cannot be of benefit to them like that." DAIS asked if the UCE knew why the September 11th attacks were successful and then answered it was due to their total secrecy. DAIS instructed the UCE to plan and not leak information. DAIS further stated, "[T]hey do not need any evidence. Just a tip and a suspicion. If someone says that this belongs to a terrorist group, they will come to your house, handcuff you and take you."

34. DAIS instructed the UCE to stay away from others, not discuss this idea with others, and secure the UCE's social media account. DAIS also told the UCE that he/she must act like an ordinary person. She also advised the UCE to not act interested in these topics and if someone asked about it, the UCE should tell them these topics do not interest him/her. DAIS emphasized that total secrecy is the most important thing and that the UCE must take time in planning, choosing a target, and studying it well from all aspects, even if it takes months.

35. DAIS told the UCE it is hard to join the [Islamic] State because they do not have much land under their control and instead it is better to execute an attack where you are. DAIS suggested potential targets for attacks, such as street festivals and celebrations in the summer, or churches. DAIS also advised that it should be something that would devastate and kill more than

one person. Further, she said, "Learn how to make bombs and explosive belts as a preparation process. They've been talking about this for months." After the UCE said he/she has no experience making weapons or explosives, DAIS said, "No problem, making bombs is easy, and you can also start with poisons. I have a [social media] Channel you may benefit from." She further said, "I advise you to use poisons first" and then she again recommended her channel as a place to find an encyclopedia of poisons. DAIS told the UCE to let her know if the UCE needed help. She said the easiest poison to make is Ricin, which she claimed is very effective and lethal to the touch. DAIS then sent a link to the social media channel and said, "Lessons in making explosives and everything related to Lone Wolves, may Allah make us beneficial." DAIS then asked, "Remember Boston Marathon bombing?" The UCE responded affirmatively, and DAIS said, "It was very easy to make. All it needs is a pressure cooker, shrapnel and explosives. Join my channel and research." The UCE asked if there were any poison recipes DAIS could send to the UCE, and DAIS responded, "Yes. I will send you the poison of Ricin for it is easier, more effective, and cannot be traced, even if the person dies, it cannot be found in the body. All you need is just two items." DAIS then said, "Castor seeds and Acetone." The UCE and DAIS then exchanged email addresses.

36. On or about May 2, 2018, the UCE and DAIS exchanged private messages via Facebook. The UCE asked DAIS about her social media channel titled, "Shu'a' Al-Khilafah for lone wolves." I believe Al-Khilafah refers to the Caliphate, aka ISIS. DAIS responded by providing a new link to a social media channel and stating that the link is not publicly available to members but rather just to the administrators. The UCE's review of the channel revealed that it is directed to "lone wolves" making poisons, explosives, weapons, and silencers. I believe that "lone wolves" refers to individuals who are inspired by one or more terrorist groups to commit attacks

acting on their own. The channel has 89 members, four photos, 10 videos, 445 files and one shared link. The translated titles of the 92 documents the UCE pulled down all relate to explosives, guns, attack planning, and target selection.

37. On or about May 3, 2018, the UCE sent a private message to DAIS via Facebook account UID ending in 2186. The UCE asked if the account was the account of a variant of HE to which DAIS responded in the affirmative. The UCE said that he/she had downloaded the Ricin file from DAIS's social media channel. DAIS said, "Good. May Allah make you successful. It's easy to make but remember to be cautious." DAIS continued to provide the UCE with advice such as wearing multiple gloves and covering the surface of the work table "because it's lethal to the touch." In discussing potential targets, DAIS suggests a government post or placing it in water reservoirs. During the conversation, DAIS told the UCE that she resides in the United States. The UCE asked DAIS if it was easy to travel to the Unites States and suggested there might be more targets in the United States. DAIS agreed and said there are many opportunities in the United States. DAIS offered that they could work together. Ricin is a biological toxin made from the castor bean.

38. A review of information provided from Facebook on or about May 11, 2018, pursuant to 18 U.S.C. § 2702, identified a conversation between DAIS (using Facebook UID ending in 2942) and a Facebook user (referred to here as EAR). EAR told DAIS, "I am in need of a way to build explosives by using agricultural fertilizer." DAIS replied, "Participate in my channel about explosives" and then provided a link to her channel titled "The ray of the Khilafa- Explosives: Lone Wolves." The summary included with the link described the channel as providing "[l]essons in manufacturing of explosives and everything regarding Lone Wolves." EAR said that he would like to "build a bomb that can uproot a whole house. I am confused on which one

to pick, and don't know how to formulate in grams of explosives and how to make it powerful." DAIS advised EAR that he needed to "start with a small amount, meaning don't make the whole thing at once. You have to experiment with small quantities and then make it bigger." EAR thanked DAIS for her advice.

IDENTIFID EMAIL ACCOUNT

39. **E-mail Account practical_75@hotmail.com**: According to Twitter's response to a court order issued pursuant to 18 U.S.C. § 2703(d) on or about September 12, 2017, Twitter account 3881114854 was associated with the email address practical_75@hotmail.com. The same IP address that was used to create this Twitter account also was used to create a Facebook account that has UID ending in 8560 and display name "HEBA DAIS" and that is associated with email address practical_75@hotmail.com. The Twitter account was created in or about October 2015; the Facebook account was opened in or about November 2015. Open source online research conducted by FBI Milwaukee in or about August 2017 for the name Waheba DAIS yielded a result on the website Quanki.com. Quanki.com is described as an online data aggregator that searches for information on people within the United States. Quanki.com listed email address practical_75@hotmail.com as one of DAIS's personal identifiers. During a jail call from Waukesha County Jail to one of her children on or about June 17, 2018, DAIS instructed her child to use email address practical_75@hotmail.com to access a Facebook account that had been used by DAIS, in order to find contact information for one of DAIS's Facebook friends.

40. In general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. Even if the

subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time.

41. There is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2339B will be found in the subject ACCOUNT. In my training and experience, I know that ISIS supporters, especially those who conduct their activities online, use multiple email and social media accounts to engage in such activities, often as a way to conceal them. In this case, DAIS is believed to have used more than two dozen Facebook accounts, four of which are identified above. Accordingly, it is reasonable to assume that DAIS used the ACCOUNT in her material support activities and that relevant evidence may be found in this account.

BACKGROUND CONCERNING EMAIL

42. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("email") access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name hotmail.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft. are likely to contain stored electronic communications (including retrieved and unretrieved email for subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

43. A Microsoft subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails),

and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

44. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

45. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

46. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

47. This application seeks a warrant to search all responsive records and information under the control of Microsoft, a provider subject to the jurisdiction of this court, regardless of where Microsoft has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.[5]

48. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under

[5] It is possible that Google stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2d Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States— pertaining to the identified account that is in the possession, custody, or control of Google. The government also seeks the disclosure of the physical location or locations where the information is stored.

investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email account practical_75@hotmail.com that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, an email provider headquartered at 1065 La Avenida, Building 4, Mountain View, California (CA) 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider. The Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within ten days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2339(b) involving DAIS since March 1, 2017, including, for the account identified on Attachment A, information pertaining to the following matters:

a. Any information in any form that is related to terrorism or a threat the national security of the United States;
b. Evidence of loyalties to a foreign power;
c. Weapons, ammunition, tactical equipment, tactical or camouflage clothing, explosives, explosives devices, explosive precursor chemicals, incendiaries; incendiary devices, incendiary chemicals or precursor chemicals and any other hazardous devices or substances deemed relevant to the investigation;
d. Flags, banners, patches, specifically designed clothing that depicts the symbol of a terrorist groups or terrorist movements;
e. Forms of identification, journals, and diaries;
f. Travel documents and indicia of travel overseas and domestically, including airline tickets, passports, visas, hotel records, and travel itineraries;
g. Calendars, time schedules, address books, and contact list information;

h. Financial information to include all financial institution records, checks, credit or debit cards, automated teller machine cards, public benefit program cards, account information, other financial records, financial instruments and moneys;

i. Money orders, wire transfers, cashier's check receipts, bank statements, passbooks, checkbooks, and check registers pertaining to travel overseas, the Islamic State of Iraq and al-Sham (ISIS), terrorist or military-like activities, or violent acts;

j. Cellular telephones, smart telephones, computers, electronic data storage devices or media, associated electronic accessories;

k. Any information that could be determined to passwords, personal identification numbers (PINs), or other information necessary to encrypt or decrypt information;

l. Evidence of geographical location of the user of the identified account at times relevant to the investigation; Global Positioning System (GPS) information and mapping history from any account;

m. Secure storage facilities for financial instruments, passports, visas, and identification documents, including safe deposit boxes;

n. Persons associated with ISIS or involved in terrorist or military-like activities or violent acts overseas or in the United States, including their identities and location and contact information;

o. Organizations whose purpose, primary or ancillary, is raising, collecting, organizing, distributing, or facilitating funds, goods, personnel, or services for training and fighting overseas or in the United States and *not* in conjunction with the U.S. armed forces;

p. Instructions, in any form, relating to explosives, biological weapons, terrorist attacks, or the hacking and other unauthorized use of computers and email and social media accounts; and

q. Hacking or the unauthorized use of any computer or email or social media account.

r. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner;

s. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

t. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and

u. The identity of the person(s) who communicated with the account about matters relating to providing material support to terrorist organizations, including records that help reveal their whereabouts.